Security Policy Guidance

Version 1.2

Prepared by HR CDS TT

August 16, 2011

Revision History

Name	Date	Reason For Change	Version
HRCDSTT	18 May 2011	Document Creation	1.0
HRCDSTT	20 June 2011	Updates based on team discussions	1.1
HRCDSTT	23 June 2011	Release candidate 1, with updated diagram	1.2

Contents

List of Figures

ACRONYMS and DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Data Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SP	Security Policy

1 Introduction

This document describes the requirements for the *Security Policy document* described in the DRD. In the following, we assume that we are describing systems that

- include domains
- flows among domains that by "policy" must be strictly limited to the authorized usage
- may have provisions of service policies as well.[1].

1.1 Document Goal

The objective of the Security Policy document is to capture, in a precise way, the desired security policy for the CDS under development. The Security Policy document will be used in turn as a basis for the system's security policy model. Figure 1 denotes the relationship between the Security Policy document and the other documents described in the DRD.

The security policy document is to be derived primarily from the security objectives document as described in the DRD and the overarching organizational policy that is applicable to the system [2] [3] .

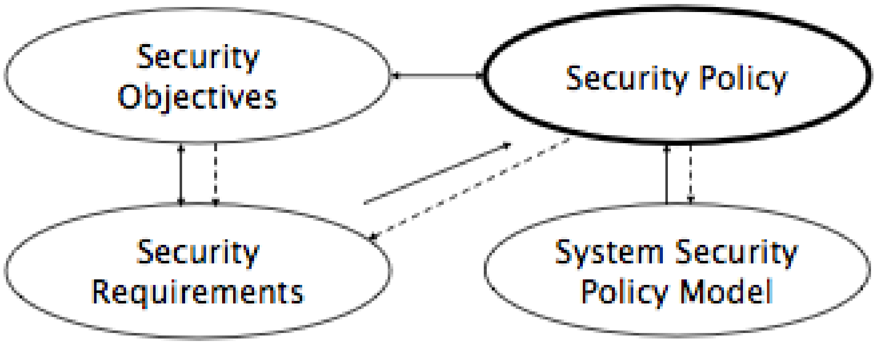

Figure 1: Relation of Security Policy document to Other Documentation

1.2 Document Contents

The developer of the Security Policy document has a large amount of flexibility regarding the form, format, and wording of the document. However, for a variety of reasons, some conventions should be followed. For example, in order to ensure

[1] This approach includes Multi-Level, Access and Transfer CDS systems

[2] For example, executive orders, DoD Policy, etc.

[3] Ideally, all appropriate governing policies will be accounted for in the security objectives document. However, in cases where appropriate policy is not cited in the security objectives, it is nonetheless necessary to update the Security Objectives document appropriately.

consinstency of interpretation amongst system evaluators, the security policy document must describe the system security policy in terms of the following properties:

- Confidentiality
- Integrity
- Availability

Furthermore, to facilitate tracability and tailoring, the following questions should be answered to gather the information in the Security Policy document:

- What are the entities and the domains of the System?
- How are the entities named?
- How are entities authenticated?
- Which flows are permitted among the domains?
- What sorts of content filtering must be applied for a given flow?
- What assumptions are being made about the environment?
- Which inter-domain information flows are explicitly permitted?
- How are access control decisions made for a given flow?
- To what extent must the system account for unintended and/or malicious use?
- What is the prioritization policy (if any) and/or the “Battle Short” policy that the CDS should support?

2 Discussion

2.1 Scope and Applicability

The system’s Security Policy document must, in plain language, characterize the sorts of security policies that the system is intended to enforce [4]. It is up to the developer to determine the appropriate scope of the security policy document for their system. More general characterizations expand the applicability of the system to a broader range of problems, but increase the level of effort required to prove and/or demonstrate assurance for the system in all such cases. In contrast, an extremely narrow and focused security policy is relatively simple to develop against, but is unlikely to be reusable in a variety of environments and/or configurations.

[4] This includes a characterization of the environments in which these policies are to be enforced.

2.2 Formality

The “Formality” of the Security Policy document depends on the Robustness Level required for the system. In general, the Security Policy document should provide enough detail that the data owners, the developers and the users of the system know what the security properties of the system should be:

- The *data owners* should know which information flows will be permitted (with all other flows prohibitied).
- The *developers* should know what the specific security properties are for each permitted data flow.
- The *users* should be aware of their expected rules of usage are, and how their actions will impact overall system security.

For CDS’s that require High Robustness, the policy should be concise, unambiguous and consistent so that it can be represented by a Formal Security Model [5].

2.3 System Monitoring, Management, and Control

Most, if not all, of the information flows supported by a CDS are among entities outside the security boundary of the CDS itself. However, many information systems that utilize CDS’s require some interaction with the CDS itself. In cases where information is sent to and/or received from the CDS regarding the status of the CDS[6], the traffic in question should still be considered an information flow with respect to the system’s security policy. As such, any information flows related to status, management, and control of the CDS should be covered by policies within the Security Policy document. Such policies should specify the CDS itself as an entity that acts as an endpoint in the information flow itself, rather than as an intermediary.

2.4 Security Domain Localization

Typically, while security domains involved in a cross domain information flow are connected to a CDS, those security domains are otherwise external to the security boundary of the CDS itself. However, in some cases, a CDS encompasses one or more security domains that are actually *internal* to the system. More specifically, a CDS may include ’internal’ domains that are connected to a controlled interface via network connections[7], or may involve virtualized ’internal’ security domains that only exist within a single CDS component. In either case, the Security Policy document must specify its policies in terms of the relevant security domains.

[5] See the **Security Model** document in this series.

[6] this includes management traffic that changes the configuration of the CDS.

[7] For example, some multilevel CDS systems involve specific controlled interfaces that mediate communications between disparate single level domains and a multilevel domain.

2.5 Granularity of Flow Definitions

Different CDS systems will support different levels of granularity of information flow policy enforcement. The Security Policy document must specify the information flow control policies for its supported flows in terms of the appropriate level of granularity. For example, a policy that governs a cross domain information flow could be at any of the following levels of specificity:

- *separate security domains*- The policy governs all information flows among the domains.
- *individual entities in separate security domains*- The policy governs information flows between explicitly defined entities within the separate security domains connected to the CDS.
- *groups of entities in separate security domains*- The policy governs information flows between a group of entities among the separate, connected security domains connected to CDS that share a particular set of properties.

If a CDS facilitates information flows at varying levels of granularity, then the appropriate level of granularity must be specified for each specific policy within the Security Policy document.

2.6 Permission and Prohibition

The purpose of a CDS is typically to control the information flow among different security domains. The CDS only permits specified information flows[8]. It is noteworthy that the policy governing information flows must cover all *potentially* permitted information flows. Information flows that are not described in the Security Policy document as permissible are implied to be prohibited in all cases. While all flows that are not permissable are implicitly denied, there is no guidance against the explicit prohibition of an information flow. For example, if a developer wants to call attention to the fact that a certain information flow must *never* be permitted, they may state a flow as prohibited as a point of emphasis and/or clarity.

2.7 System Policy Layers

In almost all cases, a CDS will be a development comprised of several different components. Furthermore, system components typically have a variety of configurations under which they can operate. As such, the policy statements must account for customization of the system. For example, there are generic CDS policies that provide for the confidentiality, integrity and availability of the information and services of domains that must be tailored for each CDS. The Security Policy document could be organized in such a way that invariant policies were organized separately from policies that are more likely to be tailored. Such a practice could be useful when a system is tailored to different environments. In such cases, a substantial portion of the Security Policy document could be

[8] For *Access* CDS, there are no flows among domains, “no flows” in this case is a “specified flow”.

reused without modification because the variable portions of the policy would be organized separately from the fixed portions [9].

3 Requirements

The requirements listed below apply to the security policy for any CDS:

SP-1: The developer shall provide a security policy for the system.

SP-2: The Security Policy document shall be based on the security objecties (as defined on the Security Objectives document based on [1]).

SP-3: The security policy shall use defined terms, and cite the sources of those definitions (e.g., CNSSI 4009, etc.)

SP-4: The policy shall describe how domains will be named.

SP-5: The policy shall describe how all external entities that use the system are identified.

SP-6: The policy shall describe how all external entities that use the system are authenticated.

SP-7: The policy shall describe the data and domain separation properties to be enforced by the system.

SP-8: The policy shall describe the potential authorized information flows among entities in the system.

SP-9: The policy shall characterize the filtering [10] mechanisms, if any, required for each and every potential information flow between disparate domains.

SP-10: The policy shall describe what is meant by 'data integrity' if data integrity policies are enforced by the CDS[11].

SP-11: The policy shall describe how data integrity will be maintained as the data is processed and/or transferred by the CDS.

SP-12: The policy shall describe the extent to which information flow events will be associated with a particular entity. [12]

SP-13: If there is an availability objective(s), the policy shall describe the expected system behavior when the CDS has exhausted or nearly exhausted its resources (for example, storage space, network bandwidth, processing limits, etc.) or component failure.

SP-14: Identify the acceptable bandwidth of covert channels in the system.

[9] For example, a system may support a configuration setting that is either "high availability" or "high integrity". In such a case, the policy could localize the impacts of this configuration setting. In contrast, if the system requires all users to be authenticated, then that policy could be localized in the static section of the document.

[10] By filtering we mean e.g. content, format, redaction, release, etc.

[11] For example, 'integrity' can refer to non-reputation, self protection, data correctness, etc. Given the ambiguity of the term, clarification of its precise meaning(s) is necessary.

[12] Information Flow events associated with, for example, accountability, attribution, non-repudiation, etc.

References and Further Reading

References

[1] HR CDS TT. Security architecture and design documentation guidance. Technical report, Unified Cross Domain Management Office, June 2011. 2